Hybridization of Steganography and Cryptography

Major Project Report submitted on fulfillment of the requirements for 4thsemester of M.Sc. in Computer Science.

Submitted by

Avishek Mitra

Aditi Bhattacharjee

Under the supervision of

Ms. Subarna Sen

Certificate

This is to certify that Avishek Mitra (roll no: 115/CSC/211030) and Aditi Bhattacharjee (roll no: 115/CSC/211027) had successfully completed the Project [Hybridization of Steganography and Cryptography] under my supervision. Throughout the duration of the project, they demonstrated exemplary dedication, commitment, and proficiency in their work.

I had the pleasure of supervising Avishek Mitra and Aditi Bhattacharjee during the Project, which involved [brief description of the project's scope and objectives].

Their contributions were significant in the successful completion of the project. They consistently exhibited a proactive approach , and demonstrated excellent problem-solving abilities when faced with challenges.

————————	————————
Project Supervisor	External examiner

Date: 06.06.2023
Place: Kolkata

DECLARATION

This is to certify that the Project report entitled "Hybridization of Steganography and Cryptography" has been submitted by us in partial fulfilment of M.Sc. degree in Computer Science during the session 2022-2023. The content of this project work in full or in parts have not been submitted to any other institute or university for award of any degree or diploma. We are fully responsible for the material used in this report if any discrepancies arise in future. Wherever we have consulted the published works (in any form) of others, it is clearly attributed. Where we have quoted from the work of others, the source is always given. We have acknowledged all the relevant sources in the report and the project is free of any form of plagiarism to the best of our knowledge. With the exception of the above this report is entirely our own work.

Date: 06.06.2023

____

Mr. Avishek Mitra
[Roll No: 115/CSC/211030, Reg No:211-1111-0376-18]

____

Ms. Aditi Bhattacharjee
[Roll No: 115/CSC/211027, Reg No: 314-1211-0124-18]

Acknowledgement

We wish to express our profound sense of gratitude to our project supervisor Ms. Subarna Sen, for her support, inspiration and guidance. She has showed us different ways to approach the problem. We have also learned from her that an approach needs to be persistent to accomplish the goal. We are immensely grateful to her for giving her valuable time and constant advice for discussing various ideas related to our project work. It is being precious learning experience for us to work under her. It gives us great pleasure to recognize the remarkable efforts, dedication, and collaborate with Ms Subarna Sen in this project. I am also grateful for the support and guidance provided by Subarna Sen Mam who is our project head. Lastly, we like to express our heartiest gratitude to our friends and to all who have directly or indirectly extended their valuable guidance and advice during the preparation of this project which will give us the continuous flow of inspiration to complete the project.

THANK YOU

Avishek Mitra

Aditi Bhattacharjee

DATE: 06.06.2023

CONTENTS :

SUBJECT **PAGE NO**

Abstract

Steganography is the art and science of concealing information within other seemingly innocent media to ensure its confidentiality. This paper explores the combination of steganography with encryption algorithms to provide enhanced security and privacy for covert communication. By integrating encryption algorithms with steganographic techniques, the hidden data becomes doubly protected, making it challenging for unauthorized parties to access or decipher the concealed information.

The proposed approach addresses the need for robust security in secret communication. It provides an additional layer of protection by leveraging encryption algorithms alongside steganography. This combination not only conceals the existence of the secret message but also ensures that even if the hidden information is detected, it remains unintelligible without the proper decryption key.

The results demonstrate the effectiveness and robustness of the hybrid approach. The combination of steganography and encryption algorithms provides a secure and inconspicuous communication channel for transmitting sensitive information. The integration of encryption ensures the confidentiality of the hidden message, while steganography disguises its presence, making it resistant to detection by adversaries.

1.Introduction

1.1 Domain description

With the rapid growth of digitization, providing security to information over Internet is most challenging. Three major security goals include Confidentiality, Integrity and Availability. Confidentiality is probably the most important among three. Maintaining confidentiality of information by protecting it from malicious actions is a major challenge. It must be ensured that the message sent and the message received is same. Steganography and Cryptography plays a vital role in providing security to the information in transit.

The term "steganography" is derived from the Greek words "steganos" meaning "covered" or "protected," and "graphia" meaning "writing" or "drawing" also “Cryptography” is a Greek word means “secret writing”. It is an art of transforming original text to cipher text after applying some technique and makes it immune to attack.

What is Steganography?

Steganography is a technique used to hide secret information within other ordinary-looking data, such as images, audio files, or text, in a way that is not easily detectable. It's like hiding a message inside another message so that only the intended recipient knows it exists. The goal is to make the hidden information blend in seamlessly with its surroundings, making it difficult for anyone else to notice or decipher. Steganography is often used to protect sensitive data or to send covert messages securely without drawing attention.

What is Encryption and Decryption?

Encryption is the process of converting plaintext or readable data into ciphertext or unreadable data using an encryption algorithm and a secret key. It is a method of securing information by transforming it into a form that is unintelligible to unauthorized individuals. Encryption ensures that even if the encrypted data is intercepted or accessed without authorization, it remains confidential and cannot be understood without the corresponding decryption key.

Decryption, on the other hand, is the reverse process of encryption. It involves taking the ciphertext and applying the decryption algorithm and the correct decryption key to transform the data back into its original plaintext form. Decryption allows authorized individuals to access and understand the encrypted data.

What is Cryptography?

Cryptography is the practice of securing communication by converting information into a form that is unintelligible to unauthorized individuals. It involves techniques and algorithms that ensure confidentiality, integrity, authentication, and non-repudiation of data.

Advantages of combining steganography with encryption algorithm

Combining steganography with an encryption algorithm offers several advantages for secure communication and data protection.

Here are the key advantages:

Enhanced Confidentiality: By encrypting the data before embedding it within the carrier medium, the sensitive information remains confidential even if the hidden data is discovered. The encryption ensures that only authorized individuals with the decryption key can access and understand the hidden information.

Covert Communication: Steganography hides the existence of communication by concealing the encrypted data within the carrier medium. This covert approach makes it difficult for unauthorized individuals to detect the presence of hidden information, enhancing the privacy and security of the communication.

Added Layer of Security: The combination of steganography and encryption provides an additional layer of security. Even if an attacker detects the presence of the carrier medium, they would still need to overcome the encryption to access the concealed data. This dual-layered protection makes it more challenging for unauthorized parties to compromise the information.

1.2 Motivation :

The motivation behind combining steganography with an encryption algorithm is to enhance the security and covert communication of sensitive information. Here are the key motivations in brief:

Increased Confidentiality: By encrypting the data before embedding it within a carrier medium using steganography, the hidden information remains confidential even if the carrier is intercepted or accessed by unauthorized individuals. The encryption ensures that the concealed data is unintelligible without the corresponding decryption key, providing an additional layer of protection.

Covert Communication: Steganography focuses on hiding the existence of communication, making it appear as inconspicuous as possible. By combining it with encryption, the hidden information is not only concealed but also rendered unreadable. This combination ensures that the communication remains covert, minimizing the chances of detection or suspicion.

Dual-Layered Security: The combination of steganography and encryption provides a two-layered security mechanism. Steganography obscures the presence of the encrypted data, making it difficult to detect, while encryption ensures the confidentiality of the hidden information. Unauthorized individuals would have to overcome both the steganographic hiding technique and the encryption to access the sensitive data, significantly increasing the level of security.

Defense against Attacks: Combining steganography with encryption adds complexity and challenges for attackers. Even if an attacker detects the presence of steganography, they would still need to decipher the encrypted data to access the information. This dual-layered approach makes it more challenging for attackers to compromise the confidentiality of the hidden information.
In summary, combining steganography with an encryption algorithm provides heightened confidentiality, covert communication, dual-layered security, and defense against attacks.

1.3 Scope of the project :

The scope of combining steganography with an encryption algorithm involves researching, developing, and implementing techniques to securely hide encrypted data within carrier media.

This work encompasses:

Algorithm Development: Designing and developing steganographic algorithms that can effectively embed encrypted data into carrier media while maintaining the integrity and imperceptibility of the carrier.

Security Analysis: Evaluating the robustness and security of the combined steganography and encryption system against various attacks, such as statistical analysis, brute-force attacks, or detection algorithms.

Integration and Implementation: Integrating the steganography and encryption algorithms into a cohesive system or software solution that allows users to easily encrypt data and embed it into carrier media. This may involve creating user-friendly interfaces and tools.

Performance Optimization: Optimizing the performance of the combined system to ensure efficient embedding and extraction processes, minimizing any potential impact on the carrier media or overall system performance.

Practical Applications: Exploring the practical applications of the combined steganography and encryption system, such as secure communication channels, confidential data storage, or digital watermarking.

Security Considerations: Addressing potential vulnerabilities and risks associated with the combination of steganography and encryption, such as key management, authentication, and the impact of attacks on the carrier medium.

2.Background

In the last few years, the researchers have shown the impact of Steganography and Cryptography on the real life events and needs in their research activities. Moreover, a notable amount of works have been proposed in the related fields to monitor the effect of the same.
We have reviewed some of the articles and works as per our Project interest.

1.Hide and seek: An introduction to steganography .[1]

2.An overview of image steganography. [2]

3. Cryptography and network security .[3]

4.High Capacity data hiding using LSB Steganography and Encryption.[4]

5.Image steganography techniques: an overview.[5]

6.Image based steganography and cryptography.[6]

7.A review on steganography and cryptography. [7]

3.Methodology

3.1 PROBLEM FORMULATION :

Nowadays weak encryption or the absence of encryption can make data more vulnerable to unauthorized access or interception. Without robust encryption or steganography, personal privacy can be compromised. Communication, including emails, messages, or file transfers, can be intercepted and monitored, violating individuals' privacy rights and confidentiality.

The problem addressed in this project is the need for secure communication and data protection. While encryption algorithms provide confidentiality by transforming data into unreadable form, there is still a risk of the encrypted data being detected or targeted by attackers. Additionally, the act of encryption itself may attract attention, potentially compromising the confidentiality of the communication.

The objective of this project is to investigate and develop a solution that combines steganography with encryption algorithms to address these challenges. The goal is to hide encrypted data within a carrier medium in a way that is imperceptible, ensuring confidentiality of the communication.

3.2 Algorithm Description

Pixel difference Steganographic algorithm

Pixel difference steganography is a technique that hides information within the differences between adjacent pixels in a digital image. Instead of modifying the pixel values directly, this approach focuses on manipulating the variations between neighboring pixels.

The basic idea behind pixel difference steganography is to encode the secret message by altering the differences between consecutive pixel values. This technique takes advantage of the fact that small changes in pixel differences are often imperceptible to the human eye.

Steganographic encoding algorithm :

```
1. Convert the image into greyscale and store it in img.
2. For each character of the text do the following
    2.1. Convert the ASCII value of the character into an 8-bit binary equivalent
    2.2. For each bit do the following
        2.2.1. Calculate the absolute difference between the present and next pixel value of img row-wise.
        2.2.2. If the difference is odd and the bit is 0, then decrement the value of the next pixel by 1.
        2.2.3. Else if the difference is even and the bit is 1, then increase the value of the next pixel by 1.
        2.2.4. Increment the (next, present) pointer of the matrix by 1.
        2.2.5.If the value of the next pointer is equal to the number of columns of the image matrix then set present pointer to the first column and next pointer to the 2nd column and increase the row by 1.
    2.3. End for .
3. End for.
4.End.
```

Steganographic decoding algorithm:

```
1. Took the image as img.
2. Start with an empty string 'text' to store the decoded message.
3. Initialize 'msg' as an empty string to store the binary representation of the differences between adjacent pixels.
4. Initialize 'l' as 0 to keep track of the length of msg.
5. Initialize ch as an empty string to store the decoded character.
6.Iterate over each row of the image using the outer loop:
    6.1.Iterate over each column (except the last column) of the image using the inner loop.
        6.1.1.Calculate the absolute difference between the present and next pixel value of img row  wise.
        6.1.2. Increment 'l' by 1.
        6.1.3.Check if 'l' reaches 8 (indicating a complete 8-bit character):
        6.1.4.Append the character to ‘text’.
        6.1.5Reset msg to an empty string and rese ‘l’ to 0.
        6.1.6.Check if the decoded character is the null character '\0' (indicating the end of the message):then break
    6.2. End for.
7.Check if the decoded character is the null character '\0' (indicating the end of the message):then break
8. End for.
9. Return the decoded message ‘text’.
```

Vowel Text Encryption (VTE)- The Proposed Encryption Method

VTE uses a (5 X 8) matrix for storing uppercase English alphabets. The idea is to share this (5 X 8) matrix publicly. An index number is assigned to each row and column and a secret key is generated using this index numbers. Index number for each row and column ranges between '00' to '99'. Index values are not repeated for row and column. Firstly, a (5 X 8) matrix is constructed using the proposed Matrix Construction algorithm. A string of integers is formed starting from index of first column to fifth, followed by index of first row to eighth. This string of integers is the agreed upon secret key between the sender and the receiver. This key i.e., the row and column index numbers will change in each round; following the proposed Key generation algorithm.

Sender encrypts the plaintext following the proposed encryption algorithm and using the key generated for each round. Receiver, at the receiving end, decrypts the ciphertext following the proposed decryption algorithm and using the same secret key.

(5 X 8) matrix Construction:

1. Fill the matrix column wise starting from the first column and fill the first place with 'A'.
2. Repeat step 1 until the next vowel is encountered.
3. Repeat step 1 and 2 until all the letters in English alphabet are visited once.
4. Fill the last two rows using numbers ranging from '0' to '9'.
5. Fill the blank cells with 'α', 'β', 'γ' and 'Φ' respectively.

	A	E	I	O	U
	B	F	J	P	V
	C	G	K	Q	W
	D	H	L	R	X
	α	β	M	S	Y
	γ	ɸ	N	T	Z
	0	1	2	3	4
	5	6	7	8	9

Table 1.1: VTE (5 X 8) Matrix

Key Generation Algorithm:

1. Assign any random 2-digit integer ranging between ‘00’ and ‘99’ to the first column.

2. Repeat step-1 and fill up all the column indices without repeating and column index value.

3. Assign any random integer ranging between ‘00’ and ‘99’ to every row index without repetition.

4. Initial key for each round is generated by placing the assigned values of the column indices followed by the values of the row indices (Table 1.2).

5. Represent this key in bit stream (Column numbers and row numbers will be represented using 8 bits).

6. Perform 1-bit cyclic left shift in this total bit stream.

7. Divide 104 bits, starting from MSB, into 13 sub parts each containing 8 bits.

8. Perform mod 100 operations if any number in 13 sub parts exceeds 99.

9. Represent 13 sub streams as 2 digit integer.

10. If any number in the 13 sub streams repeated; keep adding 1 to it until a new number gets generated.

11. This stream of 13 integers is the key for the next round. First five 2-digit integers in the stream are column indices and the next eight 2-digit integers are row indices.

12. Generate 103 different keys by repeating step-5 to step-11 for each round.

13. Use a new initial key and repeat similar steps to continue second round key generation.

The Encryption Algorithm

1. Add ‘α’ as the starting character of the plaintext.

2. Add ‘β’ as the ending character of the plaintext.

3. Add ‘ϕ’ to indicate the space between the words.

4. Divide the plaintext into sub parts, each containing 8 characters.

5. If any sub part has lesser than 8 characters, fill it with ‘γ’ to make the length

6. Different keys generated in each round are used to encrypt the text of each sub-part.

7. Replace each character in the plaintext with its corresponding column index followed by its row index to generate the cipher text.

The Decryption Algorithm

1. Divide the cipher text into sub parts. Each sub-part consists of 32 digits.

2. Further subdivide each 32 digits into 8 sub parts, each containing 4 digits.

3. In each subpart of 4 digits, first 2 digits represent column number and the next 2 digits represent row number.

4. Replace each of these 4 length strings with the element present in the corresponding column index and row index.

5. For first 32 digits initial key will be used for decryption, for next 32 digits second key will be used and so on.

4. Implementation

To implement our project we have done a few steps. For implementing our algorithms we use Python as a programming language.

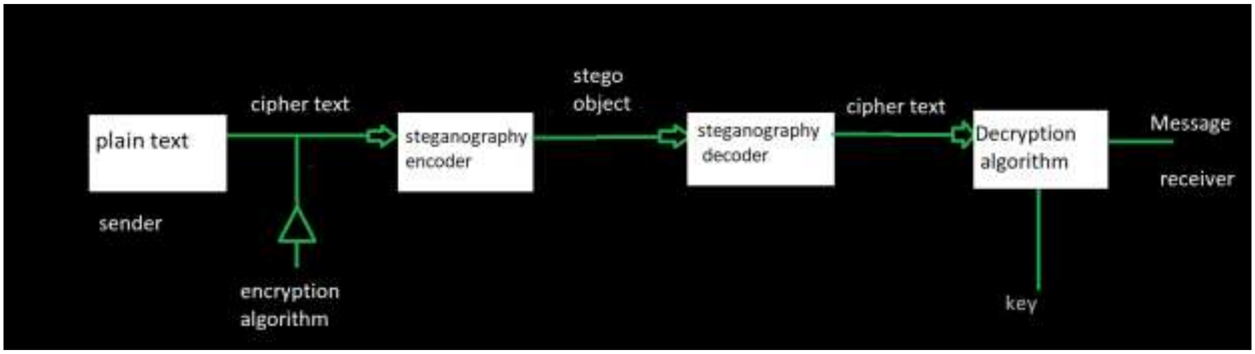


Figure 1

Process:

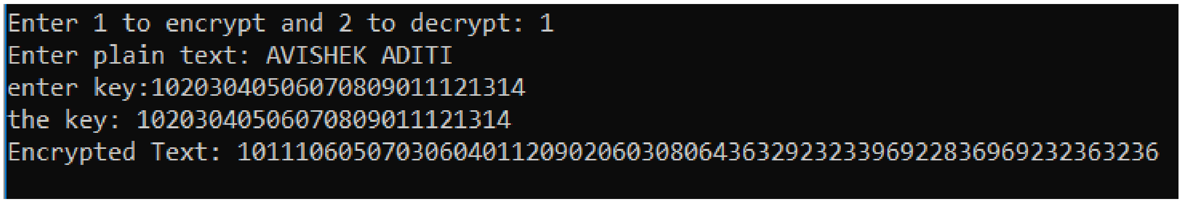
1. At first, Sender writes the message which he/she wants to send to the receiver.
2. Then we choose our Vowel text encryption algorithm to encrypt our message.
3. Using a private key we finally decrypt our message.
4. Then select our carrier medium which is an image for embedding the encrypted data.
5. Then use our Steganographic encoding technique to hide the cipher text in the image.
6. After the encrypted data is successfully embedded within the carrier medium, the resulting steganographic object is stored securely.
7. After sending the steganographic object to the receiver, we use our Steganographic decoding technique to get the encrypted data.
8. Then using our private key to decrypt the encrypted message.
9. Finally, the receiver gets the actual message which is sent by the sender.

5. Result and Discussion

Sender side:

Encrypt the data:

1. Write the message which we want to send.
2. Write the private key for encryption.
3. Finally, the plain text is transformed into the cipher text.

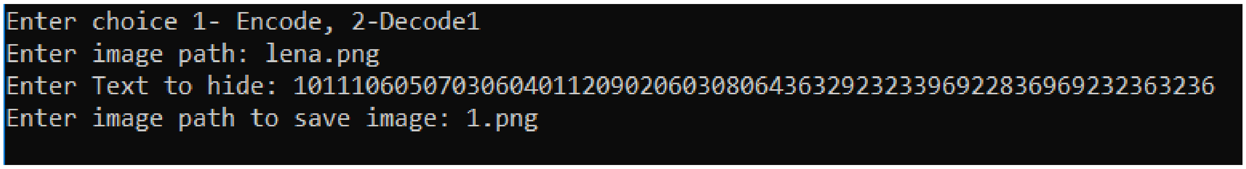


```
Enter 1 to encrypt and 2 to decrypt: 1
Enter plain text: AVISHEK ADITI
enter key:102030405060708090111213 14
the key: 1020304050607080901112131 4
Encrypted Text: 1011106050703060401120902060308064363292323396922836969232363236
```

Figure 2

Embed the Encrypted Data:

1. Choose the image where we want to hide the cipher text.
2. Then put the cipher text to hide it.
3. Select a name for the steganographic image and store it.



```
Enter choice 1- Encode, 2-Decode1
Enter image path: lena.png
Enter Text to hide: 1011106050703060401120902060308064363292323396922836969232363236
Enter image path to save image: 1.png
```

Figure 3

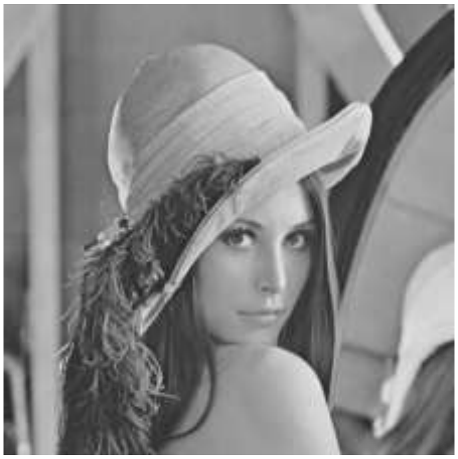


Figure 4

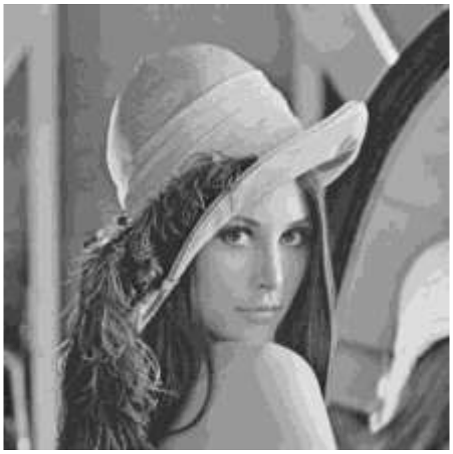


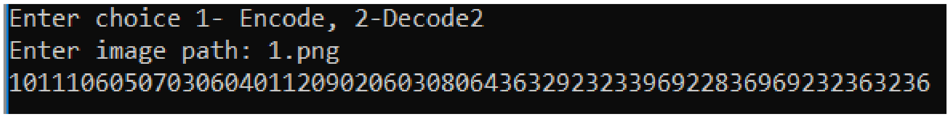
Figure 5

Figure 4 is the image that is selected as a medium and Figure 5 is the image that is generated after the steganographic technique.

Receiver side:

Steganographic decoding:

1. Choose the image which the receiver gets and using Steganographic decoding get the cipher text.

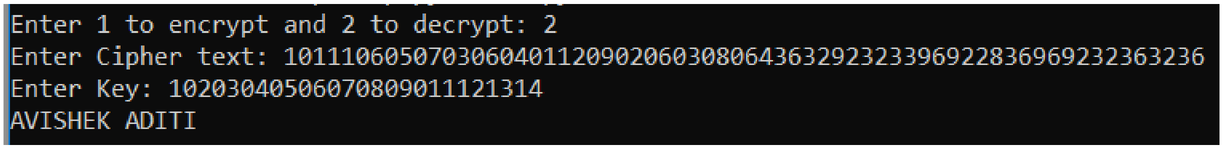


```
Enter choice 1- Encode, 2-Decode2
Enter image path: 1.png
101110605070306040112090206030806436329232339692283696923236323
```

Figure 6

Decryption:

1. Enter the cipher text which we get in the previous step.
2. Enter the private key to decrypt the cipher text.
3. Finally, we got the actual message which is sent by the sender.



```
Enter 1 to encrypt and 2 to decrypt: 2
Enter Cipher text: 101110605070306040112090206030806436329232339692283696923236323
Enter Key: 10203040506070809011121314
AVISHEK ADITI
```

Discussion:

After getting the result by using our own steganography and encryption algorithm we can say that our technique maintains confidentiality in better form.

encoding the data only in LSB is now a little bit easy to retrieve it. So our new approach can make it more difficult and provide more security to hide our data in the image. For this, the out image has a very minor difference from the input image.

In our proposed algorithm, Key Size is calculated by multiplying the number of rows and the number of columns by 8. Here, the number of rows is 5 and the number of columns is 8; summing to 13. Each index is represented using 8 bits. So, the total number of bits used to represent the key becomes 104 bits (13 X 8 bits).

The combination of steganography and encryption provides an additional layer of security to protect sensitive information. The implemented solution ensures that the encrypted data is concealed within a carrier medium, making it difficult for unauthorized individuals to detect or access the hidden information.

6. Conclusion

Our project “Hybridization of Steganography and Cryptography” has provided us with a powerful solution for secure communication and data protection. By combining steganography and encryption, we have achieved enhanced security and stealthiness in our communication system.

Through the implementation process, we have successfully embedded encrypted data within carrier media using steganographic techniques. This approach has allowed us to hide the encrypted information in a covert manner, making it difficult for unauthorized individuals to detect or access the hidden data.

7. References

[1] Provos, Niels, and Peter Honeyman. "Hide and seek: An introduction to steganography." *IEEE security & privacy* 1, no. 3 (2003): 32-44.

[2] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "An overview of image steganography." In *ISSA*, vol. 1, no. 2, pp. 1-11. 2005.

[3] Forouzan, B. A., & Mukhopadhyay, D. (2011). Cryptography and network security (Sie). McGraw-Hill Education.

[4] Laskar, Shamim Ahmed, and Kattamanchi Hemachandran. "High Capacity data hiding using LSB Steganography and Encryption." *International Journal of Database Management Systems* 4, no. 6 (2012): 57.

[5] Hamid, Nagham, Abid Yahya, R. Badlishah Ahmad, and Osamah M. Al-Qershi. "Image steganography techniques: an overview." *International Journal of Computer Science and Security (IJCSS)* 6, no. 3 (2012): 168-187.

[6] Bloisi, Domenico Daniele, and Luca Iocchi. "Image based steganography and cryptography." In *VISAPP (1)*, pp. 127-134. 2007.

[7] Mishra, Rina, and Praveen Bhanodiya. "A review on steganography and cryptography." In *2015 International Conference on Advances in Computer Engineering and Applications*, pp. 119-122. IEEE, 2015.